INDONESIAN TREASURY REVIEW
JURNAL PERBENDAHARAAN, KEUANGAN NEGARA DAN KEBIJAKAN PUBLIK

MANAJEMEN RISIKO KEAMANAN INFORMASI PADA SISTEM APLIKASI KEUANGAN TINGKAT INSTANSI (SAKTI) KEMENTERIAN KEUANGAN

Eko Supristiowadi
Direktorat Jenderal Perbendaharaan
Yudho Giri Sucahyo
Universitas Indonesia

Alamat Korespondensi: ecxo.doc@gmail.com

INFORMASI ARTIKEL

Diterima Pertama
05 Mei 2017

Dinyatakan Diterima
28 Maret 2018

KATA KUNCI
SAKTI, manajemen risiko keamanan informasi, ISO 27005, NIST SP 800-30

KLASIFIKASI JEL
O300

ABSTRAK

The aim of this study is to make information security risk management for SAKTI. The reason behind the study is SAKTI still does not have any tool to ensure the availability and continuity of SAKTI services. In order to make information security risk management for SAKTI, this study using the guidelines from several framework such as of ISO 27005 and NIST SP 800-30. The output of this study is the security risk management information for SAKTI, that contains process of risk identification, selection of controls to mitigate risk, and acceptance of risk by risk owners.

Penelitian ini bertujuan untuk menyusun manajemen risiko keamanan informasi Sistem Aplikasi Keuangan Tingkat Instansi (SAKTI). Hal yang melatarbelakangi dilakukannya penelitian ini adalah karena SAKTI belum memiliki perangkat yang dapat memastikan keberlangsungan dan ketersediaan layanan SAKTI. Penelitian ini menggunakan beberapa standar seperti ISO 27005 dan NIST SP 800-30. Keluaran dari penelitian ini adalah sebuah manajemen risiko keamanan informasi SAKTI, yang di dalamnya terdapat proses identifikasi risiko, pemilihan kontrol untuk memitigasi risiko, dan penerimaan risiko oleh pemilik risiko.

1. PENDAHULUAN

Salah satu wewenang Menteri Keuangan dalam pengelolaan keuangan negara adalah menetapkan sistem akuntansi dan pelaporan keuangan negara. Berdasarkan Peraturan Presiden Nomor 71 tahun 2010 tentang Sistem Akuntansi Pemerintah, yang di dalamnya ditetapkan bahwa penerapan akuntasi berbasis akrual paling lama 4 (empat) tahun setelah Tahun Anggaran 2010, maka terdapat kewajiban bagi Menteri Keuangan untuk menyukseskan penerapan akuntansi berbasis akrual selambat-lambatnya tahun 2015.

Atas kewajiban ini, Kementerian Keuangan membuat sebuah langkah untuk mengakomodasi terlaksananya sistem akuntansi berbasis akrual. Langkah yang dilakukan untuk menyukseskan penerapan akuntansi berbasis akrual adalah dibuatnya sebuah program bernama Program Reformasi Penganggaran dan Perbendaharaan Negara atau RPPN, yang tertuang di dalam Keputusan Menteri Keuangan Nomor 72/KMK.05/2009 tentang Program Reformasi Penganggaran dan Perbendaharaan Negara.

Adapun salah satu manfaat Program RPPN sebagaimana yang tertuang di dalam KMK Nomor 72/KMK.05/2009 adalah terwujudnya tahapan transisi penerapan sistem akuntansi dari basis kas ke akrual. Salah satu cara yang kemudian ditempuh untuk dapat merealisasikan manfaat tersebut adalah berupa pembentukan Tim RPPN yang tertuang di dalam Keputusan Menteri Keuangan Nomor 203/KMK.01/2010 tentang Tim RPPN. Di dalam Tim RPPN terdapat Tim Kortek, yaitu Tim Koordinasi Teknis yang melibatkan beberapa unit Eselon I di Kementerian Keuangan, antara lain Ditjen Anggaran, Ditjen Perbendaharaan, dan Sekretariat Jenderal Kementerian Keuangan (PUSINTEK). Tim Kortek bertugas untuk melakukan koordinasi dan evaluasi dalam penyusunan, implementasi, dan monitoring reformasi sistem perbendaharaan dan anggaran, khususnya dalam rangka pelaksanaan pengembangan Sistem Perbendaharaan dan Anggaran Negara (SPAN), seperti yang tertuang di dalam SK Tim Kortek terakhir di tahun 2015, guna mendukung penerapan akuntansi berbasis akrual.

Menurut Sudarto (2012), SPAN adalah bagian dari *Integrated Financial Management Information System* (IFMIS), dan melalui IFMIS pengelolaan keuangan mulai dari *budget process*, *budget execution process*, sampai dengan *the accounting and reporting process* dapat terotomasi menggunakan sebuah sistem atau aplikasi. Selain aplikasi SPAN, terdapat aplikasi lain yang dikembangkan dalam kaitannya dengan pengembangan SPAN yaitu Sistem Aplikasi Keuangan Tingkat Instansi (SAKTI), yang diperuntukkan bagi *spending unit* atau dalam hal ini Satuan Kerja Kementerian Negara/Lembaga.

Aplikasi SPAN dan SAKTI adalah aset sistem informasi yang penting bagi Kementerian Keuangan. SPAN dan SAKTI menjadi penting karena kedua aplikasi tersebut berkaitan erat dengan pengelolaan APBN, mulai dari perencanaan hingga pelaporan. Tidak berfungsinya aplikasi SPAN dan SAKTI dapat berimplikasi pada tidak cairnya dana APBN, baik untuk pembiayaan proyek, operasional Kementerian, sampai kepada pembayaran gaji pegawai negeri. Selain dapat berdampak pada proses pencairan dana, hal penting lain yang dapat terdampak atas tidak berfungsinya SPAN dan SAKTI adalah pelaporan keuangan berbasis akrual yang tidak dapat dilaksanakan.

Melihat peran penting dari aplikasi SPAN dan SAKTI tersebut, maka perlu ada mekanisme yang dapat membuat aplikasi SPAN dan SAKTI selalu tersedia untuk digunakan. Menurut Gibson (2011) salah satu mekanisme yang dapat dilakukan agar aset informasi tetap tersedia pada saat akan digunakan adalah dengan penerapan manajemen risiko keamanan informasi.

Berdasarkan latar belakang tersebut, maka sebagai langkah awal penelitian, dilakukan pengumpulan fakta di lapangan terkait pelaksanaan manajemen risiko di SPAN dan SAKTI. Berdasarkan observasi di Direktorat Sistem Informasi dan Teknologi Perbendaharaan (SITP) Ditjen Perbendaharaan, dan Pusat Sistem Informasi dan Teknologi Keuangan (PUSINTEK), Setjen Kementerian Keuangan, yang dilakukan selama kurang lebih 1 bulan, diperoleh fakta bahwa pada aplikasi SPAN telah diterapkan manajemen risiko, yang tertuang di dalam dokumen Matriks Risiko dan Pengendalian SPAN, sementara pada SAKTI belum ditemukan adanya pelaksanaan manajemen risiko.

Adanya fakta bahwa SAKTI belum memiliki manajemen risiko, penelitian ini dilakukan dengan tujuan untuk membuat manajemen risiko khususnya terkait keamanan informasi yang sesuai dengan kebutuhan SAKTI. Dengan demikian, baik data maupun aplikasinya, SAKTI dapat selalu tersedia untuk digunakan oleh organisasi yang membutuhkannya.

2. KERANGKA TEORI

2.1 Risiko dan Manajemen Risiko

Menurut Kouns dan Minoli (2010), risiko adalah kemungkinan kerugian atau kehilangan. Lebih lanjut dijelaskan bahwa risiko adalah sesuatu yang merupakan perkalian antara kemungkinan terjadi dan dampak yang

ditimbulkan dari sebuah kejadian yang tidak diinginkan. Adapun manajemen risiko, menurut Gibson (2011), adalah sebuah praktek mengidentifikasi, menilai, mengendalikan, dan memitigasi risiko.

Pendorong utama risiko adalah adanya ancaman dan kerentanan. Melalui manajemen risiko organisasi dapat mengidentifikasi ancaman dan kerentanan yang ada dan mengambil tindakan yang tepat untuk mengantisipasinya, sehingga dapat mengurangi potensi kerugian yang timbul dari adanya risiko. Manajemen risiko bukan bertujuan untuk mengeliminasi risiko, akan tetapi menurunkan nilai risiko dengan menerapkan pengendalian yang sesuai, sehingga risiko dapat diterima oleh organisasi.

2.2 Informasi

Menurut ISO (2005), informasi merupakan aset penting bagi organisasi seperti halnya aset-aset lain yang dimiliki sebuah organisasi. Informasi dapat berwujud dalam berbagai bentuk. Apapun bentuk informasi, atau bagaimanapun informasi tersebut disampaikan atau disimpan, harus terjaga dan terlindungi.

2.3 Keamanan Informasi

Menurut Whitman dan Mattord (2012) keamanan informasi adalah mekanisme untuk melindungi kerahasiaan, integritas, dan ketersediaan aset informasi, baik dalam penyimpanan, pengolahan, maupun transmisi. Kemanan risiko dapat tercapai melalui penerapan kebijakan, pendidikan, pelatihan dan kesadaran, serta teknologi.

2.4 Proses Manajemen Risiko Keamanan Informasi

Proses manajemen risiko keamanan informasi yang dilakukan pada penelitian ini menggunakan proses manajemen risiko yang terdapat di ISO 27005. Berikut ini adalah penjabaran dari masing-masing proses manajemen risiko keamanan informasi yang ada di ISO 27005.

a. *Context Establishment*
Penetapan konteks manajemen risiko keamanan informasi berisi mengenai kriteria dasar penilaian risiko, ruang lingkup dan batasan, dan organisasi manajemen risiko.

b. *Risk Assessment*
Penilaian risiko terdiri dari kegiatan identifikasi aset, identifikasi ancaman, dan identifikasi kerentanan. Risiko yang telah teridentifikasi kemudian diurutkan sesuai nilai prioritas yang didapat dari matriks risiko.

c. *Risk Treatment*
Dalam rangka untuk mengurangi dampak atau kemungkinan dari risiko yang telah diidentifikasi, maka langkah selanjutnya yang harus dilakukan adalah menerapkan kontrol. Terkait proses penerapan kontrol, penelitian ini menggunakan proses mitigasi risiko yang terdapat di NIST SP 800-30. Adapun kontrol yang diterapkan dapat bersifat *preventive* atau *detective*.

d. *Risk Acceptance*

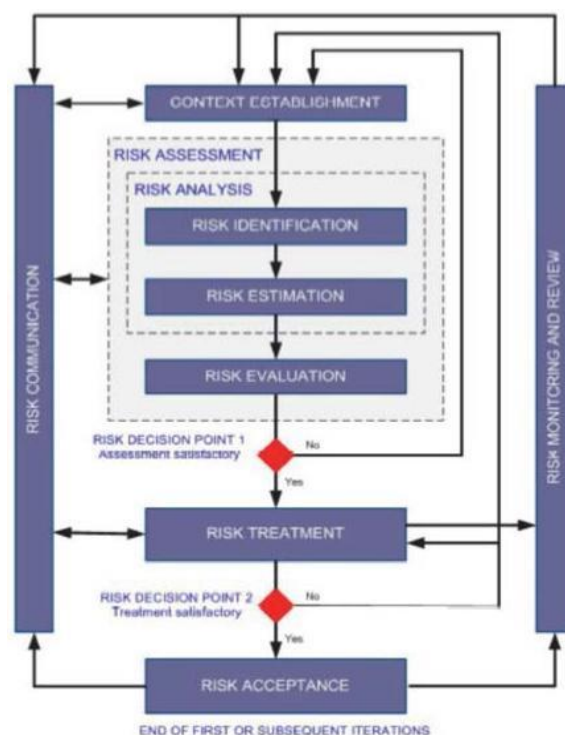
Proses untuk menerima risiko berdasarkan selera risiko dari pemilik risiko, baik dengan penetapan kontrol maupun tidak.

e. *Risk Communication*

Sharing informasi terkait risiko yang telah diidentifikasi, yang dilakukan oleh pemilik bisnis terhadap seluruh *stakeholder* yang memiliki kaitan dengan bisnis yang ada.

f. *Risk Monitoring and Review*

Kegiatan yang berkesinambungan untuk terus mengidentifikasi kerentanan, dan ancaman, yang dari waktu ke waktu mengalami perubahan

Gambar 1. Manajemen Risiko Keamanan Informasi ISO 27005

Sumber: ISO, (2011)

2.5 Standar Penyusunan Manajemen Risiko Keamanan Informasi

Terdapat beberapa standar yang dijadikan panduan dalam menyusun manajemen risiko keamanan informasi SAKTI. Berikut ini adalah

beberapa standar tersebut:

a. ISO 27001
Menurut *International Organization for Standardization* (ISO), ISO 27001 adalah standar yang berisi mengenai persyaratan yang dibutuhkan dalam penyusunan sistem manajemen keamanan informasi.

b. ISO 27002
Menurut *International Organization for Standardization* (ISO), ISO 27002 adalah standar yang memberikan panduan untuk standar keamanan informasi organisasi dan praktik pengelolaan keamanan informasi termasuk pemilihan, implementasi dan pengelolaan pengendalian dengan mempertimbangkan lingkungan risiko keamanan informasi organisasi.

c. ISO 27005
Menurut *International Organization for Standardization* (ISO), ISO 27005 adalah standar yang berisi panduan dalam menyusun manajemen risiko keamanan informasi.

d. NIST SP 800-26
Menurut *National Institute of Standards and Technology (NIST),* NIST SP 800-26 adalah standar yang berisi pertanyaan untuk kegiatan *self assessment* di sebuah organisasi. *Self assessment* tersebut bertujuan untuk mengetahui status terkini dari program keamanan informasi di sebuah organisasi.

e. NIST SP 800-30
Menurut *National Institute of Standards and Technology (NIST*), NIST SP 800-30 adalah standar yang berisi panduan untuk melakukan penilaian risiko di sebuah organisasi.

f. NIST SP 800-53
Menurut *National Institute of Standards and Technology (NIST)*, NIST SP 800-53 adalah standar yang berisi mengenai prosedur penilaian keamanan informasi sekaligus kontrol keamanan yang dapat diterapkan di sistem informasi dan organisasi.

2.6 Perbandingan Standar Manajemen Risiko Keamanan Informasi

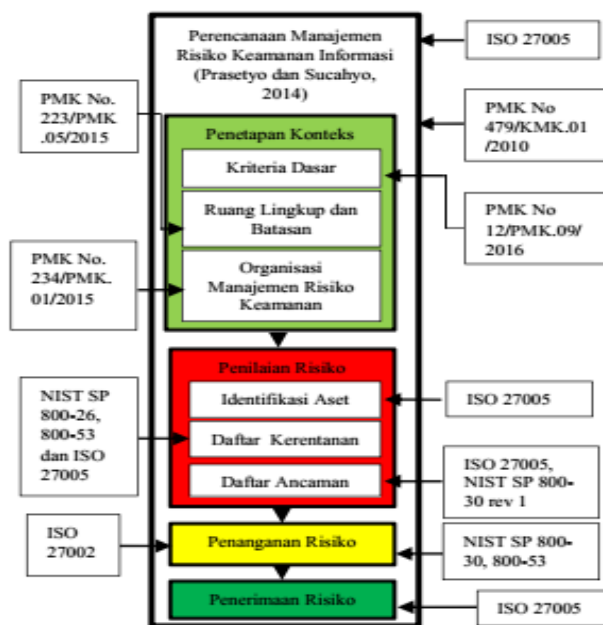
Sebelum diputuskan standar manajemen risiko keamanan informasi yang akan digunakan dalam penelitian ini, terlebih dahulu dilakukan perbandingan berbagai standar manajemen risiko keamanan informasi yang ada. Adapun hasil perbandingan standar dalam penelitian ini dapat dilihat pada Tabel 1.

Tabel 1. Perbandingan Standar Manajemen Risiko Keamanan Informasi

	Standar			
	COSO	RMF	ISO 27005	NIST SP 800- 30
Area	Organisasi secara keseluruhan	Aktivitas SDLC	Khusus terkait keamanan informasi TI	Khusus terkait keamanan informasi TI
Alur atau komponen pelaksanaan manajemen risiko	Ada 8 komponen manajemen risiko, dan lebih bersifat sebagai pengendalian	Ada 3 fase pelaksanaan manajemen risiko kerja	Ada 8 komponen manajemen risiko	Ada 9 langkah penilaian risiko dan tujuh langkah perencanaan mitigasi risiko
Keseuaian dengan Manajemen Risiko Keamanan Informasi	Teknologi Informasi termasuk di dalam ERM, namun tidak dibahas secara detail	Lebih kepada manajemen risiko pada sisi SDLC	Terkait dengan manajemen risiko keamanan informasi	Berisi penilaian risiko dan mitigasi risiko teknologi nformasi

2.7 Kerangka Teoritis

Berdasarkan studi literatur yang dilakukan, maka dapat disusun kerangka teoritis penelitian sebagaimana terlihat pada gambar 2.

Gambar 2. Kerangka Teoritis

Penjelasan atas kerangka teoritis di atas adalah sebagai berikut:

1. ISO 27005 dan PMK Nomor 479/KMK.01/2010 digunakan sebagai dasar dalam menyusun Manajemen Risiko Keamanan Informasi SAKTI.
2. Untuk setiap proses penyusunan manajemen risiko, berikut adalah dasar yang digunakan terkait proses-proses tersebut:
   a. Penetapan Konteks
   Di dalam proses penetapan konteks, terdapat beberapa subproses yang menjadi bagian dari penetapan konteks, yaitu:
   - Kriteria Dasar
     Dalam menentukan kriteria dasar, digunakan PMK Nomor 12/PMK.09/2016 sebagai dasar penyusunan.
   - Ruang Lingkup dan Batasan
     Penentuan ruang lingkup dan batasan, menggunakan PMK Nomor 223/PMK.05/2015 sebagai dasar.
   - Organisasi Manajemen Risiko Keamanan Informasi
     Dasar yang digunakan dalam membuat organisasi manajemen risiko keamanan informasi adalah PMK Nomor 234/PMK.01/2015.

   b. Penilaian Risiko
   Di dalam penilaian risiko, terdapat beberapa subproses di dalamnya, yaitu:
   - Identifikasi Aset
     Dalam mengindentifikasi aset, standar yang digunakan sebagai panduan adalah ISO 27005.
   - Daftar Kerentanan
     NIST SP 800-26, NIST SP 800-53, dan ISO 27005 digunakan sebagai panduan dalam mengidentifikasi kerentanan pada SAKTI.
   - Daftar Ancaman
     Daftar Ancaman diambil dari beberapa contoh ancaman yang ada di standar ISO 27005, dan NIST SP 800-30 Revision 1.

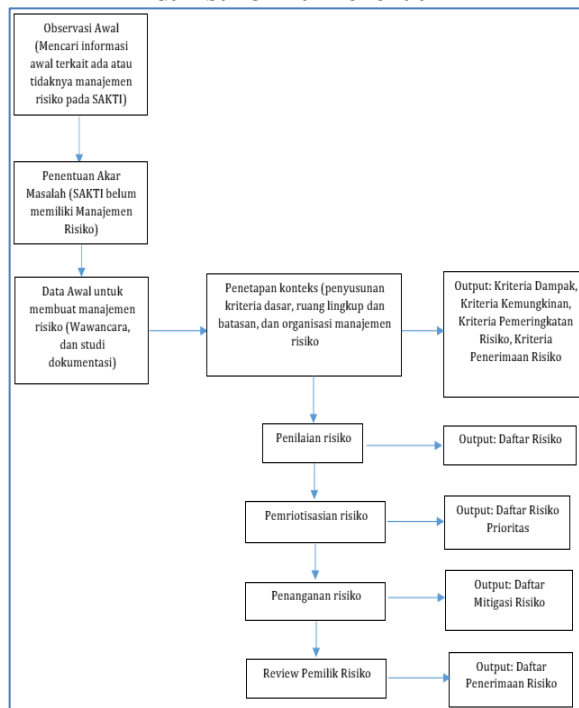
   c. Penanganan Risiko
   Dalam menerapkan penanganan pada risiko yang telah diidentifikasi, standar yang dijadikan panduan adalah ISO 27002, NIST SP 800-3, dan NIST SP 800-53.

   d. Penerimaan Risiko
   Penerimaan risiko adalah batas toleransi sebuah risiko dapat diterima oleh pemilik organisasi, baik setelah mendapat penanganan atau tanpa perlu penanganan.

3. METODOLOGI PENELITIAN

3.1 Alur Penelitian

Alur penelitian dari penelitian ini terdapat pada Gambar 3.

Gambar 3. Alur Penelitian

Penjelasan alur penelitian adalah sebagai berikut:

1. Kegiatan awal yang dilakukan dalam penelitian ini adalah melakukan observasi di Direktorat Sistem Informasi dan Teknologi Perbendaharaan (SITP) Ditjen Perbendaharaan, khususnya pada Subdit Pengelolaan Sistem Informasi Eksternal (PSIE), dan Pusat Sistem Informasi dan Teknologi Keuangan (PUSINTEK), Setjen Kementerian Keuangan. Observasi dilakukan kurang lebih selama 1 bulan untuk mengetahui ada tidaknya pelaksanaan manajemen risiko pada SAKTI.
2. Berdasarkan hasil observasi awal yang dilakukan dan diketahui bahwa SAKTI belum memiliki manajemen risiko, maka penelitian ini mengangkat masalah tentang belum adanya manajemen risiko pada SAKTI.
3. Langkah berikutnya dalam penyusunan manajemen risiko keamanan informasi SAKTI adalah pengumpulan data. Beberapa cara yang dapat digunakan untuk mengumpulkan data yaitu wawancara, dan studi dokumentasi (Yin, 2011).
   Beberapa pihak yang menjadi narasumber dalam wawancara yang dilakukan pada penelitian ini antara lain:
   a. Kasubdit Pengelolaan Transformasi Teknologi Informasi (PTTI), Dit. SITP.
   Informasi yang diperoleh dari wawancara dengan Kasubdit PTTI Dit. SITP adalah terkait dengan pelaksanaan manajemen proyek SAKTI.
   b. Kasubdit Pengelolaan Sistem Informasi Eksternal (PSIE), Dit. SITP.
   Informasi yang diperoleh dari wawancara

dengan Kasubdit PSIE Dit. SITP adalah terkait dengan ada atau tidaknya manajemen risiko pada SAKTI, dan seberapa penting manajemen risiko SAKTI perlu dibuat jika ternyata SAKTI belum memiliki manajemen risiko.

c. Kepala Subbagian Manajemen Risiko dan Kelangsungan TIK PUSINTEK
Informasi yang diperoleh dari wawancara dengan Kasubbag Manajemen Risiko dan Kelangsungan TIK PUSINTEK adalah terkait penerapan manajemen risiko di *Data Center* (DC) dan *Disaster Recovery Center* (DRC) Kementerian Keuangan, yang merupakan lokasi *hosting* aplikasi SAKTI.

d. Staf Operasional Subbagian Manajemen Risiko dan Kelangsungan TIK PUSINTEK
Informasi yang diperoleh dari wawancara yang dilakukan adalah kepastian bahwa SAKTI belum memiliki manajemen risiko.

4. Setelah pengumpulan, langkah awal penyusunan manajemen risiko keamanan informasi adalah penentuan kriteria dasar, ruang lingkup dan batasan, serta organisasi manajemen risiko.
Output dari langkah awal ini adalah kriteria dampak, kriteria kemungkinan, kriteria pemeringkatan risiko, kriterian penerimaan risiko, ruang lingkup dan batasan, dan organisasi manajemen risiko.

5. Berdasarkan kriteria dasar yang telah disusun, yang selanjutnya dilakukan adalah melakukan penilaian risiko.
Penilaian risiko dimulai dari identifikasi aset, identifikasi kerentanan, dan identifikasi ancaman. *Output* dari langkah ini adalah daftar risiko.

6. Dari daftar risiko yang ada, kemudian dilakukan evaluasi atas risiko-risiko tersebut. untuk kemudian ditentukan risiko mana saja yang menjadi risiko prioritas. *Output* dari langkah pemrioritisasian risiko ini adalah daftar risiko prioritas.

7. Terhadap risiko yang telah teridentifikasi dan diprioritaskan, langkah yang dilakukan kemudian adalah menerapkan kontrol guna mengurangi dampak dan kemungkinan risiko yang ada. *Output* dari penerapan penangangan risiko ini adalah daftar mitigasi risiko.

8. Proses yang berikutnya dilakukan setelah menerapkan kontrol risiko adalah penerimaan risiko. Proses penerimaan risiko ini melibatkan peran serta dari pemilik bisnis. *Output* dari kegiatan ini adalah daftar penerimaan risiko.

3.2 Daftar Pertanyaan

Pertanyaan yang diajukan kepada narasumber dalam penelitian ini bertujuan untuk menggali informasi mengenai kerentanan/kelemahan yang terkait dengan SAKTI.

Adapun daftar pertanyaan disusun menggunakan panduan standar NIST SP 800-26. NIST SP 800-26 adalah standar yang berisi mengenai panduan *self assessment* keamanan informasi pada teknologi informasi.

Terdapat tiga *domain* besar pembagian daftar pertanyaan yang terdapat di dalam NIST SP 800-26, yaitu:

1. *Management Control*
Management control fokus pada manajemen sistem keamanan teknologi informasi dan manajemen risiko pada sistem.
Pada *management control*, terdapat lima sub*domain* pertanyaan, yaitu:
   a. Risk Management
   Risk Management fokus pada penilaian risiko. Pada sub*domain risk management* ini, terdapat ± 11 pertanyaan terkait risiko.
   b. Review of Security Control
   Review of Security Control fokus pada pelaksanaan evaluasi berkala terkait penanganan risiko. Pada sub*domain review of security control* terdapat ± 8 pertanyaan.
   c. Life Cycle
   Life Cycle fokus pada siklus sistem teknologi informasi. Pada sub*domain life cycle* terdapat ± 27 pertanyaan.
   d. Authorize Processing
   Authorize Processing fokus pada keamanan pada sebuh sistem. Pada sub*domain authorize processing* terdapat ± 11 pertanyaan seputar otorisasi.
   e. System Security Plan
   System Security Plan fokus pada perencanaan terkait pemenuhan kebutuhan keamanan sebuah sistem. Pada sub*domain system security plan* terdapat ± 6 pertanyaan.
2. *Operational Control*
Operational control fokus pada mekanisme yang terutama diterapkan dan dilaksanakan oleh staff/pegawai. Pada *operational control*, terdapat sembilan sub*domain* pertanyaan, yaitu:
   a. Personnel Security
   Personnel Security fokus pada pengguna dari sebuah seistem. Pada sub*domain personnel security* terdapat ± 14 pertanyaan.
   b. Physical Security
   Physical Security fokus pada sisi infrastruktur dan fasilitas pendukung sebuah sistem. Pada sub*domain physical security* terdapat ± 26 pertanyaan.
   c. Production, Input/Output Controls

Indonesian Treasury Review Vol.3, No.1, 2018, Hal 23-33

Production, Input/Output Controls fokus pada *help desk* bagi pengguna dan prosedur penanganan media. Pada sub*domain* ini, terdapat ± 13 pertanyaan.

d. *Contigency Planning*
Contigency Planning fokus pada keberlangsungan proses bisnis organisasi pada saat terjadi gangguan. Terkait *contigency planning* terdapat ± 19 pertanyaan.

e. *Hardware and Systems Software Maintenance*
Hardware and Systems Software Maintenance fokus pada pemantauan terkait pemasangan dan *update* perangkat keras dan lunak untuk memastikan sistem berfungsi sesuai dengan yang diharapkan. Pada sub*domain* ini terdapat ± 23 pertanyaan.

f. *Data Integrity*
Data Integrity fokus pada perlindungan data dari kerusakan baik secara tidak disengaja maupun dengan sengaja. Terkait sub*domain data integrity* terdapat ± 13 pertanyaan.

g. *Documentation*
Documentation berisi uraian tentang perangkat keras, perangkat lunak, kebijakan, standar, prosedur, dan persetujuan yang terkait dengan sistem. Pada sub*domain documentation* terdapat ± 16 pertanyaan.

h. *Security Awareness, Training, and Education*
Security Awareness, Training, and Education fokus pada kesadaran keamanan, pelatihan, dan pendidikan meningkatkan keamanan. Pada sub*domain* ini terdapat ± 6 pertanyaan.

i. *Incident Response Capability*
Incident Response Capability fokus pada kemampuan organisasi untuk merespon insiden. Terkait sub*domain* ini terdapat ± 11 pertanyaan.

3. *Technical Control*
Technical control fokus pada sistem komputer yang digunakan oleh staf. Pada *technical control*, terdapat tiga sub*domain* pertanyaan, yaitu:

a. *Identification and Authentication*
Identification and Authentication adalah terkait dengan tindakan teknis yang mencegah orang yang tidak berwenang (atau proses yang tidak sah) memasuki sebuah sistem teknologi informasi. Pada sub*domain* ini terdapat ± 18 pertanyaan.

b. *Logical Acccess Control*
Logical Access Control terkait dengan mekanisme berbasis sistem yang digunakan untuk menentukan siapa atau apa yang memiliki akses ke sumber daya sistem yang spesifik dan jenis transaksi dan fungsi yang diijinkan. Sub*domain logical access control* memiliki ± 29 pertanyaan.

c. *Audit Trails*
Audit Trails terkait dengan penyimpanan catatan aktivitas sistem berdasarkan sistem atau proses aplikasi dan aktivitas pengguna. Pada sub*domain audit trails* terdapat ± 10 pertanyaan.

Secara total, jumlah pertanyaan yang terdapat di dalam NIST SP 800-26 adalah ± 255 pertanyaan, dan seluruh pertanyaan tersebut digunakan untuk menilai kerentanan/kelemahan pada SAKTI.

4. HASIL PENELITIAN

Adapun penyusunan manajemen risiko keamanan informasi pada SAKTI adalah sebagai berikut:

4.1 Penetapan Konteks

Penetapan konteks adalah proses awal yang dilakukan untuk menentukan *baseline* atau dasar dari seluruh proses penyusunan manajemen risiko keamanan informasi SAKTI. Beberapa proses penetapan konteks adalah sebagai berikut:

a. Kriteria Dasar
Menurut ISO 27005, yang termasuk kriteria dasar dalam menyusun manajemen risiko keamanan informasi adalah kriteria dampak, kriteria kemungkinan, kriteria pemeringkatan risiko, dan kriteria penerimaan risiko.
Menurut PMK Nomor 12/PMK.09/2016, beberapa kriteria dasar dijelaskan sebagai berikut:
- Kriteria dampak adalah menentukan level dampak suatu risiko dengan mengestimasikan nilai besaran dampak negatif suatu risiko untuk satu periode ke depan.
- Kriteria kemungkinan adalah menentukan level kemungkinan terjadinya suatu risiko dengan mengestimasikan nilai peluang keterjadian suatu risiko untuk satu periode ke depan.
- Kriteria pemeringkatan risiko adalah menyusun peringkat risiko dari nilai risiko tertinggi hingga ke nilai terendah
- Kriteria penerimaan risiko adalah penentuan pada nilai risiko berapa risiko dapat diterima, baik dengan penanganan maupun tanpa penanganan.

Semua kriteria tersebut, didasarkan pada selera risiko yang dimiliki oleh pemilik bisnis/risiko yang diidentikkan dengan Peratuan Menteri Keuangan Nomor 12/PMK.09/2016 tentang Penerapan Manajemen Risiko di Lingkungan Kementerian Keuangan.

b. Ruang Lingkup dan Batasan
Pelaksanaan manajemen risiko keamanan informasi pada penelitian ini dibatasi hanya untuk SAKTI.

c. Organisasi Manajemen Risiko Keamanan Informasi
Mengacu kepada PMK Nomor 12/PMK.09/2016, dan disesuaikan dengan unit yang bertanggung jawab terhadap pengembangan dan pengimplementasian SAKTI, maka organisasi manajemen risiko keamanan informasi SAKTI berada pada level eselon II. Adapun yang menjadi Ketua manajemen risiko keamanan informasi SAKTI adalah Direktur Sistem Informasi dan Teknologi Perbendaharaan.

4.2 Penilaian Risiko

a. Identifikasi aset
Aset menurut ISO 27005 dibagi menjadi dua yaitu, aset primer dan sekunder.
Aset primer adalah proses/kegiatan/bisnis utama dan informasi dari sebuah organisasi.
Aset sekunder adalah *hardware, software, network, staff, sites*, dan struktur organisasi.
Aset yang berhasil diidentifikasi terkait SAKTI adalah 14 aset primer, dan 27 aset sekunder.

b. Daftar kerentanan
Identifikasi kerentanan pada penelitian ini menggunakan daftar pertanyaan yang terdapat dalam NIST SP 800-26. Jumlah pertanyaan yang ditanyakan kepada pemilik bisnis berjumlah 219 butir.

c. Daftar ancaman
Daftar ancaman pada penelitian ini didasarkan pada daftar ancaman yang ada di NIST SP 800-30 dan ISO 27005, yang dikonsultasikan dengan pemilik bisnis.

d. Daftar Risiko
Dari identifikasi kerentanan dan ancaman yang ada, risiko yang berhasil teridentifikasi adalah 36 risiko.

4.3 Evaluasi Risiko

Evaluasi risiko adalah proses pemrioritisasian risiko. Pemrioritisasian risiko dilakukan dengan mengurutkan nilai risiko terbesar hingga terkecil. Dari total 36 risiko yang berhasil diidentifikasi, pada Tabel 2 disampaikan 25 risiko yang disusun berdasarkan prioritas risiko.

Tabel 2 Prioritisasi Risiko

No	Kode Risiko	Level Dampak	Kemungkinan	Nilai Risiko
1	R1	4	2	8
2	R15	4	2	8
3	R2	2	3	6
4	R7	3	2	6
5	R10	3	2	6
6	R11	3	2	6
7	R12	3	2	6
8	R13	3	2	6
9	R14	3	2	6
10	R27	3	2	6
11	R16	2	2	4
12	R17	2	2	4
13	R20	2	2	4
14	R24	2	2	4
15	R25	2	2	4
16	R26	2	2	4
17	R28	2	2	4
18	R29	2	2	4
19	R36	2	2	4
20	R4	1	2	2
21	R8	2	1	2
22	R22	2	1	2
23	R31	2	1	2
24	R33	2	1	2
25	R30	1	1	1

Adapun penjelasan kode risiko pada Tabel 2 adalah sebagai berikut:

1. R1 adalah risiko tidak beroperasinya SAKTI
2. R15 adalah risiko aplikasi SAKTI tidak dapat dioperasikan
3. R2 adalah risiko komputer yang mengoperasikan SAKTI tidak dapat digunakan
4. R7 adalah risiko segala dampak yang ditimbulkan dari adanya eksploitasi ancaman terhadap kerentanan
5. R10 adalah risiko kerugian negara
6. R11 adalah risiko aplikasi SAKTI tidak dapat dioperasikan
7. R12 adalah risiko data hilang, rusak, atau disebarluaskan oleh orang yang tidak bertanggung jawab
8. R13 adalah risiko kerugian negara
9. R14 adalah risiko dokumen hilang, rusak, atau disebarluaskan oleh orang yang tidak bertanggung jawab
10. R27 adalah risiko tidak beroperasinya KPPN
11. R16 adalah risiko pencurian data, aplikasi SAKTI tidak dapat dioperasikan
12. R17 adalah risiko kerugian negara, pencurian data, aplikasi SAKTI tidak dapat dioperasikan
13. R20 adalah risiko aplikasi SAKTI tidak dapat digunakan, hilang atau rusaknya data, dan kerugian negara
14. R24 adalah risiko hilang atau rusaknya data SAKTI, dan aplikasi SAKTI tidak dapat digunakan
15. R25 adalah risiko hilang atau rusaknya data SAKTI, dan aplikasi SAKTI tidak dapat dioperasikan

16. R26 adalah risiko hilang atau rusaknya data SAKTI, dan aplikasi SAKTI tidak dapat dioperasikan
17. R28 adalah risiko tidak beroperasinya KPPN
18. R29 adalah risiko tidak beroperasinya KPPN
19. R36 adalah risiko hilang atau rusaknya data, dan aplikasi SAKTI tidak dapat digunakan
20. R4 adalah risiko beberapa kegiatan pengelolaan keuangan negara tidak dapat dilakukan
21. R8 adalah risiko kerugian negara, dan aplikasi SAKTI tidak dapat dioperasikan
22. R22 adalah risiko hilang atau rusaknya data
23. R31 adalah risiko tidak beroperasinya KPPN
24. R33 adalah risiko bangunan mengalami kebakaran, dan
25. R30 adalah risiko aplikasi SAKTI tidak dapat dijalankan.

4.4 Penanganan Risiko

Setelah risiko diperingkatkan, langkah selanjutnya adalah menetapkan kontrol untuk setiap risiko yang ada. Pada penelitian ini, jenis kontrol yang diterapkan merujuk kepada NIST SP 800-30, yaitu bersifat *preventive* atau *detective*, karena SAKTI saat ini masih dalam tahap *piloting*, dan belum beroperasi secara penuh. Adapun kontrol yang diterapkan untuk masing-masing risiko didasarkan pada ISO 27002 dan NIST SP 800-53. Tabel 3 menjelaskan tentang pihak yang bertanggung jawab atau *person in charge* (PIC) penerapan kontrol.

Tabel 3 PIC Penerapan Kontrol

No	Penanggung Jawab Penerapan Kontrol	Kode Risiko
1	Subdit PSIE	R1, R15, R2, R7, R10, R11, R12, R13, R14,R27, R16, R17, R20, R24, R25, R26, R28, R29, R36
2	Subdit PI	R1, R15, R2, R7, R10, R11, R12, R13, R14, R27, R16, R17, R20, R24, R25, R26, R28, R29, R36
3	Subdit PTTI	R15, R7, R10, R11, R12, R13, R14, R27, R24, R25, R28, R29,
4	PUSINTEK	R1, R15, R2, R7, R10, R11, R12, R13, R27, R16, R17, R20, R28, R29
5	Seksi Layanan Pengguna pada Subdit PSIE	R1, R20,

4.5 Penerimaan Risiko

Proses penerimaan risiko adalah sebuah proses yang dilakukan untuk menerima risiko yang ada. Risiko yang diterima bukan saja risiko yang sesuai dengan kriteria penerimaan risiko, namun juga risiko yang memiliki nilai risiko di atas nilai penerimaan risiko yang telah dimitigasi. Penerimaan risiko diputuskan oleh pihak yang memiliki kapasitas dalam mengambil keputusan terkait risiko yang ada.

Tabel 4 Penerimaan Risiko

No	Kode Risiko	Status Penerimaan
1	R1	Dimitigasi
2	R15	Dimitigasi
3	R2	Dimitigasi
4	R7	Dimitigasi
5	R10	Dimitigasi
6	R11	Dimitigasi
7	R12	Dimitigasi
8	R13	Dimitigasi
9	R14	Dimitigasi
10	R27	Dimitigasi
11	R16	Dimitigasi
12	R17	Dimitigasi
13	R20	Dimitigasi
14	R24	Dimitigasi
15	R25	Dimitigasi
16	R26	Dimitigasi
17	R28	Dimitigasi
18	R29	Dimitigasi
19	R36	Dimitigasi
20	R4	Diterima
21	R8	Diterima
22	R22	Diterima
23	R31	Diterima
24	R33	Diterima
25	R30	Diterima

5. KESIMPULAN

Berdasarkan pembahasan yang telah dilakukan, berikut ini adalah beberapa hal yang dapat disimpulkan, yaitu:

1. SAKTI memiliki peran yang sangat penting dalam menunjang proses pengelolaan keuangan negara, sehingga menjadi sebuah keharusan agar SAKTI memiliki perangkat untuk menjamin ketersediaan layanan SAKTI. Salah satu perangkat yang dapat digunakan untuk menjamin ketersediaan layanan SAKTI adalah dengan penerapan manajemen risiko keamanan informasi.
2. Berdasarkan observasi yang dilakukan, ditemukan bahwa SAKTI belum memiliki perangkat untuk menjamin ketersediaan layanan yang ada.
3. Pada penelitian ini, perangkat yang dibuat untuk menjamin ketersediaan layanan SAKTI adalah manajemen risiko keamanan informasi.
4. Proses penyusunan manajemen risiko keamanan informasi pada SAKTI berupa penetapan konteks, identifikasi aset, identifikasi kerentanan, identifikasi ancaman, identifikasi risiko, dan pemilihan kontrol terhadap risiko, berpedoman pada ISO

27005, NIST SP 800-26, NIST SP 800-53, dan NIST SP 800-30.

5. Penyusunan manajemen risiko keamanan informasi SAKTI yang dilakukan pada penelitian ini telah berhasil mengidentifikasi 25 skenario risiko, dan menetapkan pihak yang bertanggung jawab untuk memitigasi risiko yang ada.

6. KETERBATASAN

Terdapat beberapa keterbatasan dalam penelitian ini, sehingga disarankan pada penelitian selanjutnya untuk melakukan hal hal sebagai berikut:

1. Perlu dilakukannya analisis biaya manfaat terhadap kontrol yang diterapkan.
2. Perlu dijabarkan lebih detail terkait jadwal pengimplementasian kontrol di masing-masing risiko yang ada. Pada penelitian ini, jadwal disusun secara global tanpa menyebutkan tanggal awal dan akhir.
3. Perlu dianalisis lebih lanjut terkait dengan risiko residu. Pada penelitian ini, risiko residu tidak dianalisis lebih lanjut karena pemilik bisnis yang saat ini menjabat sebagai pihak yang bertanggung jawab atas SAKTI, menerima semua risiko residu yang ada.

DAFTAR PUSTAKA

Albertetti, F., & Stoffel, K. (2012). From Police Reports to Data Marts: a Step Towards a Crime Analysis Framework. *5th International Workshop on Computational Forensics, Tsukuba*, 48-59.

Direktorat Sistem Perbendaharaan. (2013). *Modul Spending Review - Modul Penyuluh Perbendaharaan Edisi 2013.* Jakarta: Direktorat Sistem Perbendaharaan.

Giordano, A. (2011). *Data Integration Blueprint and Modelling: Techniques for a Scalable and Sustainable Architecture.* Boston: IBM Press.

Inmon, W. (2005). *Building The Data Warehouse Fourth Edition.* Indianapolis: Wiley Publishing.

Kanwil Ditjen Perbendaharaan Provinsi Kepulauan Riau. (2015). *Kajian Fiskal Regional Provinsi Kepulauan Riau Tahun 2015.* Tanjungpinang: Kanwil Ditjen Perbendaharaan Provinsi Kepulauan Riau.

Kementerian Keuangan. (2015). Peraturan Menteri Keuangan Nomor 234/PMK.01/2015 Tentang Organisasi dan Tata Kerja Kementerian Keuangan.

Kimball, R., & Ross, M. (2013). *The Data Warehouse Toolkit: the Definitive Guide to Dimensional Modelling Third Edition.* Indianapolis: Wiley.

Kusek, J., & Rist, R. (2004). *Ten Steps to a Results-Based Monitoring and Evaluation System. .* Washington, DC: The World Bank.

Liu, X., & Luo, X. (2010). A Data Warehouse Solution for e-Government. *International Journal of Research and Reviews in Applied Sciences 4(1)*, 101-105.

Menteri Keuangan. (2015). Peraturan Menteri Keuangan Republik Indonesia Nomor 234/PMK.01/2015 Tentang Organisasi dan Tata Kerja Kementerian Keuangan.

Mundy, J., & Thornthwaite, W. K. (2011). *The Microsoft Data Warehouse Toolkit With SQL Server 2008 R2 and the Microsoft Business Intelligence Toolset Second Edition.* Indianapolis: Wiley Publishing, Inc.

Poz, M., Gupta, N., Quain, E., & Soucat, A. (2009). *Handbook on Monitoring and Evaluation of Human Resources for Health.* Geneva: World Health Organization.

Rainardi, V. (2008). *Building a Data Warehouse With Examples in SQL Server.* New York: Apress.

Reeve, A. (2013). *Managing Data In Montion: Data Integration Best Practice Techniques and Technologies.* Waltham: Morgan Kaufmann.

Republik Indonesia. (2013). Peraturan Pemerintah Republik Indonesia Nomor 45 Tahun 2013 Tentang Pelaksanaan Anggaran Pendapatan dan Belanja Negara.

Republik Indonesia. (2015). *Peraturan Menteri Keuangan Nomor 234/PMK.01/2015 Tentang Organisasi dan Tata Kerja Kementerian Keuangan*. Jakarta: Kementerian Keuangan.

Republik Indonesia. (2015). *Pokok-pokok Proses Penyusunan Anggaran Belanja Kementerian Negara/Lembaga.* Jakarta: Direktorat Jenderal Anggaran.

Sarka, D., Lah, M., & Jerkic, G. (2012). *Implementing Data Warehouse With Microsoft SQL Server 2012.* California: Microsoft Press.

Seah, B., & Selan, N. (2014). Design and Implementation of Data Warehouse with Data Model using Survey-based Services Data. *2014 Fourth International Conference on Innovative Computing Technology (INTECH)*, 58-64.

Sherman, R. (2015). *Business Intelligence Guidebook: From Data Integration to Analytics.* Waltham: Morgan Kaufmann.

The Data Management Association. (2009). The DAMA Guide To The Data Management Study Body of Knowledge (DAMA-DMBOK Guide). New Jersey: Technics Publications, LLC.

United Nations Development Programme. (2002). *Handbook on Monitoring and Evaluating for Results.* New York: UNDP Evaluation Office.

Vermooy, R., Qiu, S., & Juanchu, X. (2003). *Voices For Change: Participatory Monitoring and Evaluation in China. Kunming.* Yunnan Science and Technology Press.

Wijaya, R., & Pudjoatmodjo, B. (2015). An Overview and Implementation of Extraction-Transformation-Loading (ETL) Process in Data Warehouse (Case Study: Department of Agriculture). *2015 3rd International Conference on Information and Communication Technology (ICoICT)*, 70-74.